the right may correspond to a different input which causes the SIM card or IC to perform another different action.

[0063] As another example, a user may originate a call via the antenna **116** to a remote destination (e.g., via cellular communication technologies) and a predetermined phone number by simply shaking or tapping the mobile device. This allows the user control the operations of the mobile device and certain applications residing therein by simply moving or shaking the mobile device. This may allow the creation of a mobile communication device that does not necessarily need a handset or keypad. In other words, the SIM card of the mobile device may be handset independent and can simply be controlled by the shaking or tapping of the mobile device and subsequent detection of motion by the directional sensing mechanism **208**.

[0064] FIGS. **3** and **4** depict an alternative mechanism that may be used to protect sensitive data stored on an RFID device **108**. More specifically, rather than "enabling" the RFID device **108** to transmit sensitive data only when a predetermined motion or sequence of motions is detected by a sensing mechanism **208**, it may be possible to employ a card carrying device **304** that generates an active cancellation field **308** which is intended to distort any data transmission of the RFID device **108**. More specifically, the holder **304** may comprise a separate antenna and IC that are adapted to be activated when carried into an RF field. If an RFID device **108** is also in the holder when an RF field is applied thereto, both the antennae in the holder and an antenna in the RFID device **108** will attempt to transmit messages. The signal transmitted by the holder **304** is used to create noise thereby making it difficult or impossible to retrieve the data transmitted by the RFID device **108**. If a user desires to have their RFID device read by a reader, the user is traditionally required to remove the RFID device **108** from the holder **304** so that the cancellation field **308** is not generated.

[0065] Embodiments of the present invention propose incorporating a sensing mechanism **208** in the holder **304** rather than the RFID device **108** so that privacy protection techniques described herein can be used to protect data on older legacy RFID devices **108** that do not have a directional sensing mechanism **208**. In accordance with at least some embodiments of the present invention, a user can allow data from the RFID device **108** to be read by moving the holder **304** in a predetermined motion or sequence of motions to temporarily deactivate the cancellation field **308**. This allows the RFID device **108** to be the only antenna which responds to the reader. This can all be accomplished without requiring a user to remove the RFID device **108** from the holder **304**.

[0066] As can be seen in FIG. **4**, the holder **304** may have a preferred geometry for physically securing the RFID device **108**. The directional sensing mechanism **208** may be provided on a printed circuit board or the like that resides on the back side of the card holder **304**. The directional sensing mechanism **208** may operate in a normal fashion, but instead of enabling operations of the holder **304** when a predetermined motion or sequence of motions is detected, the directional sensing mechanism **208** may disable operations of the holder **304** for a predetermined amount of time.

[0067] With reference now to FIG. **5**, an exemplary motion table **500** used to translate motions into actions will be described in accordance with at least some embodiments of the present invention. As can be seen, rotational movements across one, two, or three axes may be used to protect data on an RFID device **108** or at least control the operation of the RFID device **108**. Additionally, sliding movements may also be considered as a motion input. When a predetermined motion or sequence of motions is detected, an action is performed in conformity with the actions listed in the table **500**. As one example, the motion or sequence of motions may result in an action which allows the RFID device **108** to transmit sensitive data to a reader. As another example, the motion or sequence of motions may result in the generation and transmission of a predetermined message. As yet another example, the motion or sequence of motions may cause the IC **204** to translate the motions into binary data which can be transmitted as a password to the reader **104** alone or in addition to other sensitive data stored on the RFID device **108**. The reader **104** can then analyze the password to determine if user access is permitted. The password may be used as a metaphor or substitution of a user input which would otherwise need to be provided to a keypad on the reader **104**. Accordingly, a reader **104** without a keypad can test what the user is carrying as well as what the user knows, thereby resulting in a substantially more secure facility.

[0068] In accordance with at least some embodiments of the present invention an enrollment process is provided whereby a user is allowed to define their personal motion or sequence of motions that will be used to protect the data on the RFID device **108**. In one embodiment, the user may be allowed to sit in front of a reader connected to a computer providing the user with a Graphical User Interface. The reader may prompt the user to enter their motion-based password and will then wait for the detection of a motion or series of motions. Once the user has performed the desired motion(s), the user may indicate that they are done and the reader/computer will replay the detected motion or sequence of motions and ask the user if that is their desired password. If the user selects yes, then the entries in the table **500** may be updated accordingly. Also, the password data may be provided back to the RFID device **108** or at least an affirmation is sent to the RFID device **108** indicating that the last motion or sequence of motions corresponds to a password entered and recognized by the reader.

[0069] In accordance with at least some alternative embodiments of the present invention, the motion-based password may also be used to protect non-RF devices. As an example, an RSA card may be secured with a directional sensing mechanism **208** performing operations as described herein. Unless a predetermined motion or sequence of motions is detected at the RSA card, then the RSA card may be prohibited from generating a code for the user.

[0070] The present invention, in various embodiments, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various embodiments, subcombinations, and subsets thereof. Those of skill in the art will understand how to make and use the present invention after understanding the present disclosure. The present invention, in various embodiments, includes providing devices and processes in the absence of items not depicted and/or described herein or in various embodiments hereof, including in the absence of such items as may have been used in previous devices or processes, e.g., for improving performance, achieving ease and\or reducing cost of implementation.

[0071] The foregoing discussion of the invention has been presented for purposes of illustration and description. The foregoing is not intended to limit the invention to the form or forms disclosed herein. In the foregoing Detailed Description